Strategy Research Project

DOD COMPUTER NETWORK OPERATIONS: TIME TO HIT THE SEND BUTTON

BY

LIEUTENANT COLONEL JOSEPH GLEBOCKI, JR.
United States Air Force

USAWC CLASS OF 2008

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **15 MAR 2008**	2. REPORT TYPE **Strategy Research Project**	3. DATES COVERED **00-00-2007 to 00-00-2008**

4. TITLE AND SUBTITLE **DoD Computer Network Operations Time to Hit the Send Button**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Joseph Glebocki Jr.**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**46**	

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

USAWC STRATEGY RESEARCH PROJECT

DOD COMPUTER NETWORK OPERATIONS: TIME TO HIT THE SEND BUTTON

by

Lieutenant Colonel Joseph Glebocki, Jr.
United States Air Force Reserve

Colonel Joseph H. Ledlow
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR:	Lieutenant Colonel Joseph Glebocki, Jr.
TITLE:	DoD Computer Network Operations: Time to Hit the Send Button
FORMAT:	Strategy Research Project
DATE:	10 March 2008 WORD COUNT: 9,702 PAGES: 46
KEY TERMS:	Defense Support to Civil Authorities, Information Operations
CLASSIFICATION:	Unclassified

The Department of Defense (DoD) is rapidly moving forward into the cyber domain of warfare, but the United States Government is not ready to exploit this evolution in Civil-Military affairs. With the United States facing new threats to its national security at home and abroad like never before, U.S. policy and law must change to enable DoD to fully defend and fight in cyberspace. Due to the highly automated and interconnected nature of U.S. critical infrastructure, it is not practical to erect a barrier between military and civilian operations that can serve U.S. national interests. Within the interagency framework, DoD should serve as the lead, including the response phase, whenever defense critical infrastructure is involved or when a cyber attack has seriously affected other national critical infrastructure. To enable this transformation, the Posse Comitatus Act (PCA) should be amended or rescinded so DoD can conduct full defensive and offensive cyberspace operations against all required targets.

DOD COMPUTER NETWORK OPERATIONS: TIME TO HIT THE SEND BUTTON

Terrorists in a cyber café in Kansas City, Missouri, infiltrate Department of Defense (DoD) computer networks and unleash a malicious virus that shuts down U.S. missile defense systems, leaving the United States vulnerable to an intercontinental ballistic missile attack. Besides defensive measures aimed at protecting its systems from further damage, DoD remains extremely vulnerable--there is not much else that it can do without the help or acquiescence of federal civilian authorities. In the meantime, lives could be lost, cities could be destroyed, and the American way of life could be changed forever. Although this is a hypothetical scenario that sounds like a science fiction thriller, such unthinkable events could happen in the future if U.S. law and policy are not changed to enable DoD to fully defend and fight in cyberspace. Clearly, DoD is moving into the cyber domain of warfare, but the U.S. Government will not be ready to exploit its full potential until DoD is given the tools and the authorities to become more aggressive in cyberspace to perform these evolving cyber missions when necessary before it is too late.

The United States' two major instruments of national power--military and economic might--are increasingly reliant upon a network of critical infrastructures and their associated cyber-based information systems. Due to advances in information technology, along with pressures to enhance efficiency in the competitive global economy, U.S. national infrastructure has become more automated and interconnected across all sectors, leaving this nation more vulnerable to physical and cyber attacks. Nowhere is this more apparent and more important than within the American military-industrial complex. The information technology revolution has changed the way business is transacted; the way government operates; and the manner in which national defense is conducted, with all three functions becoming more and more reliant upon an interdependent network of critical information infrastructures. As Department of Homeland Security (DHS) Under Secretary for Preparedness, George Forsman, stated, "Cyber security is an essential part of our preparedness efforts, because information technology systems can connect so many aspects of our economy and our society, … most importantly, our national security. Our cyber infrastructure is interwoven with our physical infrastructure, …"[1]

Legal and policy barriers against the use of DoD resources from the outset to defend and then respond to cyber attacks against U.S. national infrastructure can severely hamper its homeland security posture. With the United States facing threats to our national security at home and abroad like never before, this paper advocates that it is time to provide a new policy and legal regime for cyber offense and defense for the 21st century and beyond. It examines the cyber attack threat to U.S. critical infrastructure; discusses the impact of the Posse Comitatus Act (PCA); looks at national and DHS strategy; analyzes DoD capabilities and policies; discusses lessons learned from cyber security exercises; argues why DoD should take a more active role in the cyber defense of America; and provides recommendations for further action.

Discussion of the Cyber Threat to U.S. Critical Infrastructure

Cyberspace is a difficult concept to define since it might mean something different depending upon the context within which it is used. The official DoD definition provides that cyberspace is "the notional environment in which digitized information is communicated over computer networks."[2] Regardless of how cyberspace is defined, there can be little debate over the potential vulnerability of our networked systems. The National Infrastructure Protection Plan (NIPP) recognizes that the U.S. economy and national security are highly dependent upon the global cyber infrastructure which creates a highly interconnected and interdependent network of Critical Infrastructure/ Key Resources (CI/KR).[3] Although new technologies and interconnected networks enhance productivity and efficiency, they also serve to increase America's risk to cyber threats. For example, "[t]he expansive growth of new Internet technologies, from wireless access to voice-over-Internet telephony, has engendered new threats that have been outpacing the security responses of private and governmental users on the whole."[4] One of the great advantages of cyberspace is that it can often offer anonymity and the ability to undertake attacks remotely in an almost untraceable way, while using third party computer systems almost at will, and often with minimal risk of detection or retaliation.

Despite extensive efforts by government and private industry, the Computer Emergency Response Team (CERT) Coordination Center list of reported vulnerabilities grew from about 2,500 in 2001 to more than 7,200 in 2006, about 20 new vulnerabilities every day.[5] Similarly, an August 2005 International Business Machines (IBM) report determined that more than 237 million computer security attacks were reported worldwide in the first half of 2005 with U.S. Government organizations being the most likely target by far.[6] One can only imagine how many attacks must go undetected each and every day. Gen. James Cartwright, then STRATCOM Commander, warned in a March 2007 statement to the House Armed Services Committee that "America is under widespread attack in cyberspace. Unlike in the air, land, and sea domains, we lack dominance in cyberspace and could grow increasingly vulnerable if we do not fundamentally change how we view this battlespace."[7]

The scope of enemies in this domain is potentially limitless including traditional hostile countries trying to gain information on our military capabilities, malicious individual hackers looking to steal valuable information from the federal government, terrorists, criminal elements, and even economic competitors. Retired Gen. Barry McCaffrey stated that, "[e]very classified brief I receive underscores the absolute certainty that all our potential adversaries, terrorist organizations, and many private criminal groups conduct daily electronic reconnaissance and probes of the electromagnetic spectrum and devices which are fundamental to our national security."[8] The Federal Bureau of Investigation (FBI) even predicts that terrorists could use hackers to conduct cyber attacks to complement large scale conventional attacks.[9]

Similarly, the National Military Strategy contends that cyber attacks on U.S. commercial information systems or transportation networks could conceivably have a greater economic or psychological effect than a Weapons of Mass Destruction (WMD) attack.[10] It is well-documented that "[i]ncreasingly sophisticated use of the Internet and media has enabled our terrorist enemies to communicate, train, rally support, proselytize, and spread their propaganda without risking personal contact."[11] The National Strategy for Combating Terrorism seeks to eliminate such "cyber safehavens" because the Internet provides an inexpensive, anonymous, geographically unbounded, and largely unregulated virtual safe haven for terrorists, which can be developed anywhere in the world, regardless of where members or operatives are located.[12] These types of activities will have a much higher likelihood of success in the future if

DoD is restricted from conducting robust counterattacks and offensive operations in cyberspace.

There are countless examples of significant cyber attacks against the critical infrastructure of the United States, and there appears to be no end in sight. Furthermore, the challenges and opportunities of warfare in cyberspace are nothing new. Back in 1998, DoD set up an exercise called “Eligible Receiver” that involved the hiring of 35 hackers (government employees with no advanced intelligence) with locally purchased laptops to disrupt the U.S. response to an international crisis.[13] These hackers were able to break into the power grids of all major American cities, the “911” emergency telephone system, and the command and control networks of the Pentagon.[14]

Chinese Threat

The danger of State-sponsored threats is also growing as evidenced by the relentless activities related to China. In the fall of 2006, hackers, operating through Chinese Internet servers, launched a debilitating attack against the U.S. Commerce Department’s highly sensitive Bureau of Industry and Security, forcing it to replace hundreds of work stations and block employees from using the Internet for more than a month.[15] It was also widely recognized that the Chinese government hacked into a DoD computer system in June 2007, which forced many Pentagon computers to be taken off line for about three weeks.[16] Although the Chinese government denied supporting these attacks, an unnamed senior U.S. official stated that there was a “very high level of confidence … trending towards total certainty” that China was responsible.[17] In fact, the Naval Network Warfare Command is convinced that the predominant threat comes from

Chinese hackers, likely with government support, primarily probing DoD network targets and almost reaching the level of campaign-style, force-on-force engagements.[18]

Estonia 2007—The First Global Cyberwar?

Without most of the world even realizing it, we may have witnessed the first cyberwar in history. In May 2007, Estonia was the target of a series of "denial of service" cyber attacks which flooded national networks with fake messages and caused their servers to shut down.[19] It was very difficult to determine the exact source of the attacks since "botnets" (third party remote takeovers of computer systems) were used as part of an overall effort to protest the movement of a statute of a Communist-era Soviet soldier.[20] During the cyberspace escalation, Estonian defenses were easily breached, the attack grew exponentially, and the government had to shut down websites for days.[21] The scope of the assault resulted in Estonian networks being hit every second with four million packets of data at its peak with the attacks vectored in from more than fifty countries, many via co-opted computer systems.[22] These types of attacks had previously been experienced on a much smaller scale in China, the United States, Israel, India, and Pakistan.[23]

Impact of the Posse Comitatus Act (PCA)

Despite the growth of cyber-based threats to U.S. national security and critical infrastructure, the Posse Comitatus Act (PCA) continues to serve as a significant potential roadblock to DoD's dominance in the cyberspace domain. The PCA provides in pertinent part: "[w]hoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both."[24] In general, the statute makes it a crime for the military to execute the laws of the United States, specifically performing domestic civilian law enforcement functions.[25] Originally, the PCA prohibited the use of the Army as a posse comitatus, arising from the end of Civil War reconstruction and the conditions throughout the United States' western frontier.[26] The Act's prohibitions do not apply to members of the military reserves when not on active duty status; members of the National Guard when not in Federal service; civilian employees of DoD; the U.S. Coast Guard when not employed under DoD; or military members in an off-duty and private capacity.[27]

Legal Interpretations of the PCA

The courts have come up with at least three different legal standards when discussing potential violations of the PCA; however, there is general agreement that passive assistance to law enforcement is permitted.[28] In *United States v. Red Feather*, the District Court delineated the general standard of permissible passive roles and impermissible active roles.[29] In another case, the Court stressed whether the "use of any part of the [military] pervaded the activities of the …" federal law enforcement officers.[30] Another Federal District Court decision came up with the third standard which asks if military personnel were used to subject citizens to an exercise of military power that was regulatory, proscriptive, or compulsory in nature.[31] In addition, the courts have provided several factors that weigh against using the military in law enforcement roles including potential autonomous military rule and the loss of constitutional liberties; putting 4th and 5th Amendment protections into the hands of untrained individuals; potentially limiting the exercise of fundamental rights and creating a society dominated by fear and hostility; and the uneasiness and uncertainty that military commanders might feel.[32]

The Defense Department basically adheres to each of the three generally enunciated judicial standards on the PCA as well as any Congressional restrictions on military participation in civilian law enforcement activities.[33] However, DoD appears to specifically endorse the third test in defining permissible civil assistance activities while adding express prohibitions on direct assistance and against searches and seizures, surveillance of individuals, or acting as an undercover agent or interrogator.[34] The Justice Department's Legal Counsel uses a hybrid of the first and third tests when judging military activities against a standard of whether "there is no contact with civilian targets of law enforcement, no actual or potential use of military force, and no military control over the actions of civilian officials."[35] Furthermore, the PCA only prohibits the "willful" use of the military to execute the law so that defendants must intend to violate the Act. It is doubtful that this standard would be met when a military member acts in good faith for a perceived homeland defense mission; in an activity not viewed as law enforcement; or under a perceived exception for law enforcement activity.[36]

From a legal analysis standpoint, the jury is probably still "out" as to whether all types of DoD responsive and offensive cyberspace operations would violate the PCA. Strong arguments can be made on both sides as to whether such activities would violate the current standards. It also appears that the Department of Justice (DOJ) Standard would not be violated since there does not need to be contact with civilian targets of law enforcement; no use of military force in the traditional sense; and no military control over civilian officials. It can be further argued that the "military purpose" doctrine would be satisfied whenever the protection of DoD critical infrastructure and equipment serves as the supporting rationale. Regardless of the final conclusions of legal scholars on this topic, there is still too much uncertainty in the current state of the law to be of much value.

Exceptions to the PCA

The debate over the proper role of the military on the domestic front continues to be a hot topic since 9/11 and Hurricane Katrina. Nonetheless, the United States Congress reaffirmed its support for the PCA by stressing its continued importance and stating that it has served the nation well in limiting the use of the Armed Forces to enforce the law.[37] However, the Congress also made clear that:

> … the [PCA] is not a complete barrier to the use of the Armed Forces for a range of domestic purposes, including law enforcement functions, when the use of the Armed Forces is authorized by Act of Congress or the President determines that the use of the Armed Forces is required to fulfill the President's obligations under the Constitution to respond promptly in time of war, insurrection or other serious emergency.[38]

In fact, the statute has already been amended many times, and numerous exceptions have been created that dilute the scope of the law.

Congress has created exceptions to the PCA in four major areas: insurrections/ civil disturbances, counterdrug operations, disaster relief, and counterterrorism/ weapons of mass destruction.[39] The language of the PCA itself contains a clear exception clause for "circumstances expressly authorized by the Constitution or Act of Congress." Furthermore, there is some discretion provided to DoD in situations where an immediate response is necessary for temporary emergencies when the local authorities are overwhelmed.[40] Most importantly, statutory law provides that assistance in the context of a WMD attack may include "… use of personnel of the [DoD] to arrest persons and conduct searches and seizures with respect to violations of this section ….”[41] Even direct military assistance is permitted in limited circumstances with the two major exceptions being the “Military Purpose Doctrine” and the Insurrection Act.[42] The military purpose doctrine provides an exception if the activity in question is part of or incidental to furthering a legitimate military purpose.[43] DoD Directives further provide that the following activities are not restricted by the PCA: actions taken for the primary purpose of furthering a military or foreign affairs function of the United States; investigations and other actions related to enforcement of the UCMJ, likely to result in DoD administrative proceedings or related to a commander’s authority to maintain law and order on a military base; protection of classified information/equipment; or protection of DoD personnel and equipment.[44] Specifically, it is permissible for DoD to take action “… to protect Federal property and Federal government functions when the need for protection exists and duly constituted local authorities are unable or decline to provide adequate protection.”[45]

The PCA has consistently been weakened by laws that allow the military to help address the problems of drug trafficking, natural disasters, and terrorist attacks. Some of the PCA’s biggest changes came after President Reagan’s “war on drugs” in the 1980s. After powerful testimony by state and local leaders requesting military assistance, the Congress pushed DoD to provide indirect assistance to law enforcement including intelligence, equipment, maintenance, use of military facilities, and specialized training and tactical advice.[46] In addition to modern challenges faced by law enforcement, the President's Constitutional and statutory authorities have caused further erosion of the PCA’s prohibitions.[47] With so many exceptions already in place, is there really a need for the PCA in today's dangerous world and considering the cyberspace threat that we already face?

If the current PCA structure is maintained, a new exception should be created by Congress to allow DoD to fully defend itself against cyber attacks and properly respond to the growing threat. There exist so many other exceptions to make the PCA almost meaningless anyway. Since Congress has already provided DoD with "police powers" in the context of WMD incidents, it would not be a stretch to extend this policy to cyberspace. Although the law is still relatively new in this area, there are strong arguments that a search and seizure has taken place whenever the government conducts investigations in cyberspace relating to personal and business servers, mainframes, etc.[48] However, this is the only way for DoD to be able to protect U.S. national security interests. Such activities should be even less visible and hopefully less objectionable than having military forces on the streets during civil disturbances or conducting border patrol and counterdrug operations.

National and Department of Homeland Security (DHS) Strategy

Homeland Security has been defined as "… a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[49] The National Strategy for Homeland Security has the following strategic objectives: reducing U.S. vulnerability to terrorism, preventing terrorist attacks, minimizing any damage, and recovering from any attacks that do occur—this includes national critical infrastructure and key assets (NCI & KA) protection as a critical area.[50] Without a doubt, U.S.

Government activities in cyberspace are a key cornerstone of our national critical infrastructure efforts and a growing part of our homeland security posture.

National Critical Infrastructure Protection (CIP)

The President's Commission on Critical Infrastructure Protection (PCCIP) was created by President Clinton and charged with reviewing all physical and cyber threats to our nation's critical infrastructure.[51] In Presidential Decision Directive (PDD)/NSC-63, the President stated that "…the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[52] Under the national goals for PDD/NSC-63, it provides that "[a]ny interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."[53] The associated guidelines provide for all of the authorities, capabilities and resources of the federal government, including defense preparedness, to achieve and maintain critical infrastructure protection, with every federal department responsible for protecting its own critical infrastructure and cyber-based systems.[54]

One major challenge was the development of a system for responding to significant infrastructure attacks, while underway, with the goal of isolating and minimizing damage. The National Infrastructure Protection Center (NIPC) was supposed to provide the principal means of facilitating and coordinating the overall response, mitigating attacks, investigating threats, and monitoring reconstitution efforts, while maintaining that foreign attacks could place them in a direct support role to DoD.[55] The National Cyber Security Division (NCSD), a new part of DHS' Preparedness

Directorate, provides the federal government with a centralized cyber security coordination and preparedness function and serves as the focal point for interactions with state and local government, the private sector, and the international community regarding cyberspace vulnerability reduction.[56] Under the National Response Plan's Cyber Annex, the National Cyber Response Coordination Group (NCRCG) is designated as the main interagency mechanism to prepare for and respond to cyber incidents of national significance.[57] Among its duties,

> … the [NCRCG] leverages the capabilities of the agencies of the United States government from a cyber defense perspective, so that we have the situational awareness to detect and recognize incidents of significance. We have the ability to attribute the source of attacks and malicious activity. We have the ability for coordinated response, and we have the responsibility to help with the recovery of the disruptions that might be caused by those attacks.[58]

The National Strategy to Secure Cyberspace

Securing cyberspace is a difficult strategic challenge that requires coordinated and focused efforts from our entire society—the federal government, state and local governments, the private sector, and the American people. The National Strategy to Secure Cyberspace has three strategic objectives: preventing cyber attacks against America's critical infrastructures; reducing national vulnerability to cyber attacks; and minimizing damage and recovery time from cyber attacks that do occur.[59] It also identifies six major actions and initiatives to strengthen our national security and international cooperation including: strengthening cyber-related counterintelligence efforts; improving capabilities for attack attribution and response; improving coordination for responding to cyber attacks within the U.S. national security community; and fostering the establishment of national/international "watch" and "warning" networks to detect and prevent emerging cyber attacks.[60]

Homeland Security Presidential Directive (HSPD)-7

Another important policy document, Homeland Security Presidential Directive (HSPD)-7, establishes a national policy for federal departments and agencies to identify and prioritize CI/KR and to protect them from terrorist attacks. Some of the major difficulties with protecting these areas are the fact that most are owned and operated by the private sector, include cyber-based resources, and span all sectors of our economy. HSPD-7 provides that it is U.S. policy:

> … to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could: … impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety; undermine State and local government capabilities to maintain order and to deliver minimum essential public services; damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services; have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or undermine the public's morale and confidence in our national economic and political institutions.[61]

The Secretary of Homeland Security has the apparent responsibility to coordinate the overall national effort and to serve as the lead federal official. In addition, the Secretary is directed to maintain an organization to serve as the focal point for cyber security, with DoD and other organizations collaborating and supporting this overall mission as necessary under current law.[62] The DoD is specifically designated with lead responsibility for the defense industrial base. DHS established the United States Computer Emergency Readiness Team (US-CERT) as the 24/7 single point of contact for cyberspace analysis, warning, information sharing, and incident response and recovery operations through partnerships between DHS and the public and private sectors to protect the national cyber infrastructure and coordinate prevention/response actions to cyber attacks against the United States.[63] Furthermore, the National Infrastructure Protection Plan (NIPP) promotes cyber security by facilitating participation and partnership in CI/KR protection initiatives, leveraging cyber-specific expertise and experience, and improving information exchange and awareness of cyber security concerns.[64] The resulting framework enables security partners to work collaboratively to make informed cyber risk management decisions, define national cyber priorities, and address cyber security as part of an overall national CI/KR protection strategy.[65]

Defense Critical Infrastructure

DoD has the responsibility to assure access to defense critical infrastructure defined as "DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide."[66] Even when these resources are located at public or private sites, DoD must assure the protection of designated defense critical infrastructure (which could include civil and commercial infrastructure that provides power, communications, transportation, etc.) on a priority basis.[67] In August 2005, DoD assigned functional responsibility within the Department to coordinate with the public and private sectors to protect defense critical infrastructure from cyber attacks.[68] Finally, the President or Secretary of Defense can direct U.S. military forces to protect non-DoD assets that are of vital national significance when their incapacitation could have a serious effect on our national security.[69]

Following the current policy regime would harm our ability to meet the nation's CIP goals across the board. The DoD will not be able to swiftly eliminate all vulnerabilities to attacks upon its critical infrastructure because valuable time and effort will be lost providing intelligence to civilian officials and waiting for a bureaucratic response. DoD is supposed to be the lead for its own critical infrastructure and equipment, but it could be rendered almost helpless by the current state of affairs even when it is the direct target of dedicated cyber attacks. If foreign attacks occur, civilian agencies might even serve in a direct support role to DoD pursuant to PDD/NSC-63, but this is unlikely to happen in cyberspace under current law and policy. This system runs contrary to the National Strategy for Homeland Security, Presidential Executive Order, the DoD Strategy for Homeland Defense and Civil Support, and the National Response Plan.

Department of Defense (DoD) Capabilities and Policies[70]

In February 2003, President Bush provided classified guidance, NSPD-16, to determine how and when the United States would launch a Computer Network Attack (CNA) against foreign systems and who would be authorized to conduct such operations.[71] Due to many uncertainties in the cyberspace realm, DoD recommended that a legal review be undertaken to determine what level of cyber intrusion amounts to an actual attack; whether the response could infiltrate unknowing third party systems; and an overall framework that might apply separately to domestic or foreign attackers.[72] Clearly, there is much in the area of policy and law that must be resolved at the national and DoD levels before a final course of action can be taken. Yet, DoD officially acknowledges that cyberspace is considered a warfare domain just like air, land, sea, or space.[73]

Cyberspace is also recognized as a new theater of operations by the National Defense Strategy because successful military operations depend upon the ability to protect information infrastructure and related data.[74] However, DoD leadership knows that it will take time for our military forces to adapt to this new way of warfare since “the cyber threat is revolutionary, ... because it has no battle lines, the intelligence is intangible, and attacks come without warning, leaving no time to prepare defenses.”[75] DoD has further stated that it is building an information-centric force with networks being increasingly recognized as the operational center of gravity so it must be prepared to “fight the net.”[76] However, “[c]urrent U.S. cyber warfare strategy is dysfunctional …[as] [o]ffensive, defensive, and reconnaissance efforts among U.S. cyber forces are incompatible and don’t communicate with one another, resulting in a disjointed effort,” argued Gen. James Cartwright, former Commander of STRATCOM.[77] The Secretary of Defense has the responsibility to oversee, develop, and ensure implementation of policies, principles, standards, and guidelines for the security of information systems that support military operations.[78]

Current DoD Organization

The Unified Command Plan (UCP) assigns USSTRATCOM as the lead for DoD Computer Network Operations (CNO).[79] The Joint Functional Component Command Network Warfare (JFCC-NW) is a subordinate command of USSTRATCOM and serves as the lead for coordinating network warfare for DoD.[80] The Joint Task Force for Global Network Operations (JTF-GNO) is responsible for operating and defending U.S. worldwide information networks associated with the Global Information Grid (GIG).[81] In 1998, DoD created the JTF-CND, which later became the JTF-CNO and was realigned under STRATCOM.[82] In April 2004, STRATCOM approved a new Joint Concept of Operations (CONOPS), and the JTF-CNO transformed into its current form as the JTF-GNO when the Secretary of Defense signed a delegation of authority letter on 18 June

2004.[83] Established Computer Network Defense (CND) policy includes three tiers of response actions with corresponding levels of approval authority up to Tier 1, which includes STRATCOM being authorized to take defensive measures and actions that may “minimally and temporarily adversely affect adversary systems and may have a similar affect upon intermediate systems.”[84] However, it is apparent that CND lacks any updated policy and legal guidance to adequately guide responses to attacks against DoD networks.[85]

Although any aspects of Computer Network Attack (CNA) and its implementing organizations are likely to be highly classified, it is generally believed that the U.S. can actually destroy networks and penetrate enemy computers to take data and disable command and control networks in an interagency framework.[86] Gen. Barry McCaffrey stated that “[w]e must sort out clearly the international legal and policy considerations upon which we will base widely understood Joint Directives governing the centralized employment of offensive cyber-warfare. This is the first sword to unsheathe in time of modern combat.”[87] It has been reported that the United States did not use CNA during Operation Iraqi Freedom even though comprehensive Information Operations (IO) plans were in place, perhaps since top-level approval was not granted in sufficient time to support war objectives.[88]

It is clear that CNO mission areas are growing more important for DoD as it becomes increasingly dependent upon computer systems and networks to support our warfighters. Many of DoD’s capabilities could be degraded if adversary military groups or terrorists were able to conduct sustained cyber attacks against DoD infrastructure. Within the United States, DoD would be unable to fully defend and respond to these threats without changes to the current policy framework. Furthermore, DoD's homeland defense and homeland security missions, including "sovereignty protection" and protection of defense critical infrastructure, could be unduly hampered. DoD has invested significant manpower and resources to address the cyber-based threat with STRATCOM and its Service components primed to respond. In many cases, the DoD will have expertise that exceeds what is available in the civilian arena. Since the stakes might be so high, it does not make sense to leave the military as a reserve force or to only "break the glass" when civilian authorities make a specific request or are overwhelmed.

Accordingly, DoD should serve as the lead because its mission would be focused upon the cyber defense of defense critical infrastructure and the corresponding response, as well as responding to cyber attacks that seriously degrade other national critical infrastructure. The analogy can be drawn to defending U.S. airspace from enemy aircraft, as well as hijacked aircraft already within our airspace as demonstrated by the attacks of 9/11. There can be no differentiation between threats emanating from within and outside the United States because the risk and potential devastation are too great. Just as NORTHCOM and NORAD provide defense of our sovereign airspace with the use of Service component assets and cooperation with civil authorities, the same should be done for cyberspace. The U.S. Government will have to determine a set of protocols to enable this determination to be made in as expeditious a manner as possible. Two potential standards for DoD's cyber response are within the DoD Strategy for Homeland Defense and Civil Support and the stated policy within HSPD-7. If the New York Stock Exchange was struck by a cruise missile from another State and severely damaged, then a military response would certainly be warranted. It should be no different if a cyber attack from that same State resulted in a similar level of devastation. DoD should be able to respond in a timely and effective manner to protect and serve U.S. national interests even when the national critical infrastructure in question belongs to the private sector.

In order for the military to achieve success in the long run, the U.S. will need to develop better capabilities to determine the 2nd, 3rd, and even higher order effects of offensive cyber operations that strike targets while minimizing outside disruptions to the greatest extent possible. There are potential discrimination and proportionality issues related to the law of war that will have to be addressed as well. It will be necessary for the international community to get together and work out many of these cyber warfare issues. Even when the source location of the attack is known, there are still controversial matters that might need to be resolved. If a foreign State is the attacker, then a DoD response is certainly warranted, and DoD should always serve as the lead. In fact, PDD/NSC-63 provided that foreign cyber attacks could place the NIPC and other civilian agencies in a direct support role to DoD. Of course, it would still need to be determined what level of cyber attack can be considered an act of war or aggression by another State. If a foreign-based terrorist conducted the attack, the same rationale would apply although some might argue that the FBI or CIA should handle the response. When the actor is a domestic terrorist or U.S. citizen hacking from within our own borders, then this is the most difficult problem area to resolve due to domestic legal requirements. Nonetheless, DoD should still serve as the lead when the attack is against defense critical infrastructure or when other national critical infrastructure is seriously degraded as discussed earlier. These operations should not impact the capability of federal civilian authorities to prosecute the perpetrators in a court of law.

Military Assistance to Civil Authorities (MACA)

Employment of military forces within the borders of the United States under the heading of civil support typically falls under the broad mission of MACA which includes three main areas—military support to civil authorities (MSCA), military support to civilian law enforcement (MSCLE), and military assistance for civil disturbances.[89] DoD Directive 3025.15 establishes DoD policy and assigns responsibilities for providing military assistance to civil authorities.[90] The Directive defines MACA as "[t]hose DoD activities and measures covered under MSCA plus DoD assistance for civil disturbances, counter drug, sensitive support, counterterrorism, and law enforcement."[91] It further provides that DoD "… shall cooperate with and provide military assistance to civil authorities as directed by and consistent with applicable law, Presidential Directives, Executive Orders, and this Directive."[92]

DoD employment within the United States is supposed to be heavily weighted toward managing the consequences of the terrorist use or threat of a chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) weapon of mass destruction (WMD).[93] However, this does not appear to be the case in reality. All requests for DoD military assistance are evaluated against several criteria including: legality, the potential use of lethal force, risk to military forces, impact on the defense budget, appropriateness for a DoD mission, and any effect on military readiness.[94] DoD is supposed to always remain in support of a lead federal agency during both crisis management (FBI) and consequence management (FEMA) as delineated in the federal government's Interagency Domestic Terrorism Concept of Operations Plan and the Federal Response Plan.[95]

Under the broad MACA umbrella, it is consistent with DoD policy to move more aggressively into defensive and offensive cyber space operations. There is no likelihood of lethal force; no risk to military forces; and probably little relative impact on the defense budget and military readiness. In addition, DoD has already extended itself deeply into many areas of domestic operations such as counterdrug operations and responding to natural disasters.

Military Support to Civil Authorities (MSCA)

Military Support to Civil Authorities (MSCA) refers to DoD support provided in response to requests for assistance during domestic incidents such as terrorism, major disasters or other emergencies.[96] DoD Directive 3025.1 governs MSCA for all DoD components and defines such actions as:

> [t]hose activities and measures taken by the DOD components to foster mutual assistance and support between the DOD and any civil government agency in planning or preparedness for, or in the application of resources for response to, the consequences of civil emergencies or attacks, including national security emergencies.[97]

Military forces employed in MSCA activities shall remain under military command and control at all times and shall not perform any functions of civil government unless absolutely necessary on a temporary basis in certain emergency circumstances.[98] The Secretary of Defense has the responsibility to develop regulations to ensure that these actions do not include or permit direct participation by Service members in searches, seizures, arrests or similar activities unless otherwise authorized by law.[99]

Any military forces involved in responsive or offensive cyber activities would likely be performing such functions only when absolutely necessary on a temporary basis and in emergency circumstances. Of course, military personnel would need to be trained adequately to determine when it would be appropriate to respond to cyber attacks using some type of risk analysis and established minimum criteria such as those delineated in HSPD-7 or the DoD Strategy for Homeland Defense and Civil Support.

Military Support to Civilian Law Enforcement (MSCLE)

Military Support to Civilian Law Enforcement (MSCLE) involves military forces supporting a lead federal agency during various events including national security special events; support for combating terrorism; support to counterdrug operations; maritime security; intelligence, surveillance, and reconnaissance; and general support (i.e., training, equipping, advising).[100] It is DoD policy to cooperate with civilian law enforcement as much as possible while remaining consistent with the needs of national security and military preparedness, the historic tradition of limited direct military involvement and the requirements of applicable law.[101] In addition, the planning and execution of compatible military training and operations can take into account the information needs of civilian law enforcement when the collection is incidental to the military purpose.[102] However, any military involvement can not include direct participation in traditional law enforcement functions like searches and seizures or arrests unless otherwise authorized by law.[103]

It is arguable that DoD cyber activities would not violate the Directives regarding MSCLE when taken for the primary purpose of furthering a military function of the United States or when taken to protect classified information or DoD equipment. It is also unlikely that civilian authorities would be capable of providing an adequate response to large-scale attacks against DoD cyber-based infrastructure. There are often access or classification issues that must be dealt with so it would not make sense to hand off these problems to civilian officials. However, military members will definitely need to receive new levels of training in areas such as evidence collection for those cases when the perpetrators are subject to American criminal jurisdiction.

Lessons Learned From Cyberspace Exercises

Military and civilian authorities have recognized in the last several years that the United States faces significant challenges in the cyberspace realm, especially when diverse organizations must work together when a response is warranted. In late 2002, the city of San Antonio, Bexar County, Texas, and the surrounding region conducted an exercise, named "Dark Screen," to test the ability of local, state, and federal organizations to respond to a cyberattack.[104] In fact, "the issue of military participation continuously presented more questions than answers…" due to the PCA, numerous DoD regulations, and other federal statutes that address military support to civilian authorities.[105]

"CyberStorm," a 2006 cyber attack exercise, led by DHS, highlighted gaps and shortcomings in response planning at all levels of government.[106] Specifically, the use of classified information and networks made it increasingly difficult to coordinate among agencies, and between government and the private sector.[107] This was the first full-scale government-led cyber security exercise to examine response, coordination, and recovery mechanisms to a simulated cyber event between international, federal, state, and local governments, in conjunction with the private sector.[108] This specific scenario simulated a significant widespread cyber campaign that affected critical infrastructure elements within the energy, information technology, transportation, and telecommunications sectors.[109] The exercise had three main objectives—to disrupt specifically targeted infrastructure through cyber attacks; to hinder the government's ability to respond; and to undermine public confidence in the government's ability to provide essential services.[110] As a result, it became clear that more standard operating procedures (SOPs) and contingency plans are needed; roles and responsibilities of participants must be clarified; and more training and exercises are necessary.[111]

The CIA has also conducted its own cyber exercises in recent years. In 2005, "Silent Horizon" looked at a major cyber attack on the U.S., and it became apparent that many of the defenses are controlled by civilian telecommunications interests.[112] Another CIA-sponsored exercise, "Livewire," determined that there remained significant questions over the government's role depending on the source of the attacks—terrorists, foreign States, or private citizens.[113]

These exercises provide concrete examples of the serious issues that this nation could face under the current convoluted regime if a large-scale cyber attack took place. Valuable time would be lost as DoD and civilian officials determine their proper roles. One answer might be the use of National Guard members or civilians in each state to avoid PCA restrictions, but this would be an inefficient and unsupportable solution. Clearly, civilian and military officials need to do more together in the future to prepare and respond to the threat, but not at the cost of limiting DoD's capability to protect its mission critical systems in a timely and comprehensive fashion.

DOD Should Take a More Active Role in Cyber Defense

The cyber attack threat to U.S. critical infrastructure is well-documented within this paper and throughout many other sources. The defense critical infrastructure and other national critical infrastructure (i.e., economic, communications, transportation) of the United States are too intertwined to permit "stovepipes" across the federal government, the private sector, and elsewhere. The U.S. cannot afford to have an attack like Estonia occur that shuts down sectors of the government. In addition, the many cyber security exercises consistently show that the United States is not prepared or properly organized to meet the growing threats from States, terrorists, criminal organizations, and individual hackers.

The U.S. has made some progress with the framework laid out by the National Strategy to Secure Cyberspace, HSPD-7, the NIPP, and other relevant policy documents. In addition, significant investments have been made to build a foundation of cyberspace capabilities. DHS' NCSD, NCRCG, and US-CERT provide vital information exchange, awareness of cyber security issues, and build important partnerships. Similarly, DoD has made great strides with STRATCOM, its subordinate commands (JTF-GNO and JFCC-NW), and numerous other agencies to address the new warfighting domain of cyberspace.[114] Yet, all of these efforts may only amount to "window dressing" in the end if the PCA and current U.S. policy remain in effect.

The PCA Structure is Too Complex and Unnecessary

The PCA has been more symbolic than real as evidenced by the many exceptions permitted by Congress, the Courts' lackadaisical approach toward the statute, and the lack of federal enforcement. While the PCA has been on the books for more than 120 years, there has never been an actual prosecution for violating its provisions.[115] Leaders from the Executive and Legislative Branches have acknowledged that the current system needs to be reviewed and changes made where necessary. For example, President Bush outlined in the National Strategy for Homeland Security that "[t]he threat of catastrophic terrorism requires a thorough review of the laws permitting the military to act within the United States in order to determine whether domestic preparedness and response efforts would benefit from greater involvement of military personnel and, if so, how."[116] General Ralph Eberhart, former NORTHCOM Commander, said he "would favor changes in existing law [including the PCA] to give greater domestic powers to the military to protect the country against terrorist strikes."[117] Senator John Warner, then-Chairman of the Senate Armed Services Committee, has also stated that "the reasons for the [PCA] have long given way to the changed lifestyle we face today here in America …"[118] Clearly, there is considerable support to rescind or amend the PCA to allow DoD to take a more active role in the defense of the United States, including one of its most vulnerable domains—cyberspace.

There is a general consensus that the PCA is full of uncertainty and complexity. It is debatable when the PCA applies; what military activities are prohibited; and what are the boundaries for the exceptions that actually exist, leaving policymakers, legal practitioners, lawmakers, and military personnel confused. The confusion surrounding the PCA stems primarily from two reasons: (1) the difficulty in classifying situations as homeland defense or civil response and (2) misconceptions about the PCA due to the patchwork of legal authorities in this area.[119] It is time to rescind the PCA and replace it with a new law since it is widely misunderstood and does not provide a basis for defining civil-military relations in the current Global War on Terrorism (GWOT).[120] In critical situations like responding to nuclear terrorism or sophisticated cyber attacks, the current PCA interpretation may create a convoluted command and control structure, decreased response times, and continuity problems, leaving the federal response more vulnerable to advsersaries' exploitation.[121] The PCA is irrelevant and even dangerous to the proper use of military forces for domestic duties in the 21st century, such as cyber defense of national critical infrastructure, so it is imperative that a new law provide clear guidelines for the use of American military forces for homeland security duties and enforcing U.S. laws. One comprehensive statute could maintain the basic principles originally intended by the PCA while setting clearer lines of demarcation between permissible and impermissible DoD activities.

Lack of Civilian Capability to Respond

DoD has the responsibility to ensure that it has access to defense critical infrastructure, including DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide.[122] These are critical DoD mission areas and ones that civilian officials are often not capable of handling due to many reasons including access, classification issues, and personnel expertise. One could argue that an attack against DoD computer networks should justify a full investigation and response by DoD personnel since the actions were directed against military assets.[123] Unfortunately, DoD cannot perform these vital functions under the current legal and policy regime.

Need for Responsiveness and Speed in Cyber Space

Speed is of the essence in cyber space, but the current framework would unduly slow down any potential DoD response. A statutory exemption to the PCS is needed to alleviate the uncertainty and provide clearer guidelines to enable swift and effective action against any foreign terrorist attacks.[124] This can happen across the range of potential military operations, but it is especially prevalent in the cyber arena where degraded systems could create severe cascading effects upon our military capabilities. Even if civilian officials sit next to their DoD counterparts, there are still too many outstanding issues to provide the necessary level of speed and responsiveness.

DoD is Better Suited for Cyber Response

DoD can respond in the cyber arena in its area of expertise better than civilian authorities because it is at the core of their mission. David McIntyre, the Director of the Integrative Center for Homeland Security at Texas A&M University, stated that "[t]he Pentagon's authority trumps that of DHS in the event of an attack …[and that] the Pentagon's role in a disaster leans heavily toward response and recovery, while DHS' is more focused on prevention and mitigation."[125] Things should be no different in cyberspace. Cyber attacks need to be compared to vessels crossing into our territorial waters or tanks rolling across the Mexican border. It can be argued that any cyber attack that causes damage indistinguishable from a kinetic attack should be legally indistinguishable from more traditional military attacks.[126]

The DoD should serve as the lead when necessary since they are trained, equipped, and prepared to respond. In DoD's homeland defense role, the mission of "responding" is defined as "the ability to rapidly deter, repel, or defeat an attack."[127] If deterrence fails, the military must be prepared to rapidly respond and defend against threats including the use of preemptive or offensive actions such as computer network attack.[128] Of course, it is still important to work with and coordinate response capabilities with civilian counterparts as necessary. Furthermore, concerns that U.S. service members will serve as a substitute for civilian law enforcement can be overcome through proper guidelines and training to use the military in limited emergency circumstances.

Foreign vs. Domestic Attacks

It is often too difficult to make distinctions between foreign and domestic attacks in cyberspace so the military should be able to respond against both targets when necessary. The distinction between enemies at home and abroad has grown blurry in the age of information warfare. Specifically, this new type of homeland defense must ignore the distinction between foreign and domestic threats to be successful, a difference that is fundamental under the PCA.[129] The 2003 National Strategy to Secure Cyberspace provides that "the speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which occurs only after the fact, if at all."[130]

> [I]n most cyber attacks, the identity, location, and objective of the perpetrator are not immediately apparent. Nor is the scope of the attack ... This means it is often impossible to determine at the outset if an intrusion is an act of vandalism, organized crime, domestic or foreign terrorism, economic or traditional espionage, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to gather information from victim sites and intermediate sites such as Internet Service Providers [(ISPs)] and telecommunications carriers.[131]

Given the difficulty in determining the specific source of cyber attacks, it is arguable that, unlike responding to traditional criminal acts, the focus should be on the act itself, rather than the perpetrator, and the threshold for launching defensive and offensive actions should be lowered.[132] Many cyber security experts agree that it is hard to determine the origin of most cyber attacks due to the diffuse set up of the Internet as an attack that seems to emanate from one country could actually be controlled by another State that hijacked their networked systems through a “botnet army” or other mechanisms.[133]

Consequently, the PCA may need an additional exception carved out of the law for terrorist threats that law enforcement is not designed to handle and when probable cause exists that those involved in the attack are foreign nationals or American citizens working on their behalf.[134] Until we have the capabilities to determine the sources of cyber attacks with the utmost confidence, such a solution is probably not practical in the cyberspace realm. There are international law ramifications involved here as well, such as what constitutes self-defense in cyberspace, but these are issues that still need to be worked out. Nonetheless, the PCA forces DoD to try to delineate between foreign and domestic sources, but this is not possible with certainty in the cyber arena before it may be too late.

Offensive vs. Defensive Operations

As with foreign and domestic attacks, the distinction between offensive and defensive operations cannot be done effectively in cyberspace. There could be major issues when the notion of offensive information operations and cyberattack go beyond the typical defense context (i.e., for offensive military operations in support of a preemptive action or in response to a non-cyber attack on our national interests).[135] In order to provide a truly comprehensive cyber defense, there will be occasions when DoD will need to counterattack or shut down an adversary's cyber systems. Even defensive actions may include offensive Information Operations (IO) capabilities to disrupt adversary systems.[136] This would amount to a seizure under domestic law when a U.S.-based target is involved and a potential violation of the PCA.

Homeland Defense vs. Homeland Security

Another distinction that causes significant issues is trying to draw the line between permissible homeland defense and impermissible homeland security operations by DoD in cyberspace. DoD Joint Doctrine provides that the military supports homeland security in two ways: homeland defense and support to civil authorities with some of the relevant mission areas including: "sovereignty protection" (includes defense against computer network attack); protection of critical defense infrastructure; military assistance to civil authorities (includes CBRNE incidents); and military support to civilian law enforcement (includes combating terrorism and protecting critical national infrastructure).[137] Under the current system, the military may not be able to adequately address a terrorist attack on American soil due to the lack of clear, explicit guidelines as to when the military should act and the cumbersome bureaucratic approval process. In addition to the President being able to respond with military force to sudden attacks without Congressional approval, it is arguable that lower level commanders could do likewise when faced with defending the homeland against a terrorist attack.[138] However, terrorism is defined more as a law enforcement problem than a national security concern, and this limits the ability of DoD to counter such actions in the United States.[139]

If military activity falls under the realm of homeland defense or as part of a civil response not involving law enforcement activity, then it should be defendable under the PCA.[140] Yet, the PCA tries to make distinctions between “military attacks” and “terrorist aggression” which are more theoretical than reality-based. DoD is supposed to be the lead agency for homeland defense missions. Consistent with law and policy, the Services support combatant command requirements against all incursions that threaten our national security including computer network attack.[141] Trying to draw lines between homeland defense and homeland security missions, in an effort to satisfy the PCA’s requirements, would do more harm than good in the event of a cyber attack.

Conclusions/Recommendations

Before serious damage is done to U.S. national security through a cyber attack against DoD or other national critical infrastructure, the United States needs to re-evaluate its policy and legal framework and enable this Nation to respond to the cyber challenges that are likely to be faced in the 21st century and beyond. After what may have been the first true “cyber war” in history, perhaps supported by Russia, Estonian Defense Minister Jack Aaviksoo warned that:

> [w]e haven’t yet defined what can be considered to be a cyber attack, or what are the rights of member states and the obligations of EU and NATO in the event such attacks are launched. The EU and NATO need to work out a common legal basis to deal with cyberattacks. … how to tackle different levels of criminal cyber-activities, depending on whether what we are dealing with is vandalism, cyber terror or cyber war.[142]

A “Pearl Harbor” in cyberspace could be devastating to U.S. national security, and it should not be allowed to happen especially when it could have been prevented.

Accordingly, DoD should not only serve as the lead for the cyber defense of defense critical infrastructure, but it should also be in the lead for the response, as well as the response phase when a cyber attack has seriously affected other national critical infrastructure. This determination could be based on standards derived from HSPD-7 or the DoD Strategy for Homeland Defense and Civil Support.

In addition, the PCA needs to be amended or rescinded. The PCA has "…succeeded in putting forth an ideal, but has fallen woefully short in creating a practical, legal impediment to the use of the military for civil law enforcement."[143] The legal and policy arguments discussed in this paper conclusively show that this is the route that must be taken. Since it might be too sensitive of a political issue to do away with the PCA completely, it could be more prudent to develop a new DoD exception for cyberspace activities. Again, this exception could be based on the standards discussed earlier and derived from HSPD-7 or the DoD Strategy for Homeland Defense and Civil Support. Nonetheless, it would be very beneficial if all of the exceptions were combined with the PCA language into one comprehensive statute. Perhaps this can serve as another step toward dismantling the PCA structure if the political will exists in the future. Too bad that it's not as easy as a potential enemy's cyber attack with one finger on a keyboard—just hit the "send" button.

Endnotes

[1] DHS Under Secretary for Preparedness George Foresman, Press Conference on the "Cyber Storm" Cyber Security Preparedness Exercise, February 10, 2006, 2.

[2] Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, 12 April 2001 (as amended through 17 October 2007). There is also the more commonly used and expansive definition that cyberspace is "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." Wikipedia at http://en.wikipedia.org/wiki/ Cyberspace,

accessed October 23, 2007. It is interesting to note that Joint Publication 1-02 does not define cyber war. The author provides a conceptual definition of what could constitute a cyber war to justify a military response within this paper.

[3] Michael Chertoff, Secretary, DHS, National Infrastructure Protection Plan, 2006, 13.

[4] Peter Allor, Director of Intelligence and Special Assistant to the General Manager IBM Internet Security Systems, “Understanding and Defending Against Foreign Cyber-Threats,” Homeland Security Institute Journal of Homeland Security, August 2007, 1.

[5] Ibid., 5-6.

[6] John Rollins and Clay Wilson, “Terrorist Capabilities for Cyberattack: Overview and Policy Issues,” Congressional Research Service Report for Congress, January 22, 2007, 17.

[7] Rebecca Grant, “Victory in Cyberspace,” Air Force Association Special Report, October 2007, 3, quoting Gen. James E. Cartwright, Commander, U.S. Strategic Command, House Armed Services Committee, March 8, 2007.

[8] Gen. Barry R. McCaffrey, USA (Ret), Adjunct Professor of International Affairs, After Action Report—Nellis and Scott AFB, 14-17 August 2007, United States Military Academy, October 15, 2007, 5.

[9] Rollins and Wilson, 1.

[10] General Richard B. Myers, Chairman, Joint Chiefs of Staff, National Military Strategy of the United States of America, 2004, note 1.

[11] National Strategy for Combating Terrorism, September 2006, 4.

[12] Ibid., 17.

[13] James Adams, Chief Executive Officer, Infrastructure Defense, Inc., “Information Warfare: Challenge and Opportunity,” U.S. Foreign Policy Agenda, USIA Electronic Journal, Vol. 3, No. 4, November 1998, 1.

[14] Ibid.

[15] Alan Sipress, “Computer System Under Attack: Commerce Department Targeted; Hackers Traced to China,” Washington Post, October 6, 2006, A21.

[16] Jennifer Griffin, “Pentagon Source Says China Hacked Defense Department Computers,” FoxNews, September 4, 2007 at http://www.foxnews.com/printer_friendly_story/0,3566,295640,00.html, accessed October 28, 2007.

[17] Demetri Sevastopulo, “Chinese Military Hacked into Pentagon,” Financial Times, September 3, 2007 at http://www.ft.com/cms/s/0, accessed October 28, 2007.

[18] Josh Rogin, “Cyber Officials: Chinese Hackers Attack ‘Anything and Everything’” Federal Computer Week, February 13, 2007 at http://www.fcw.com/online/news/97658-1.html?type=pf, accessed October 28, 2007.

[19] James A. Lewis, Director, Technology and Public Policy Program, “Cyber Attacks Explained,” Center for Strategic and International Studies, Commentary, June 15, 2007, 1.

[20] Ibid.

[21] Grant, 4.

[22] Ibid., 5-6.

[23] Lewis, 1.

[24] Title 18 U.S. Code, Sec. 1385, Posse Comitatus Act (1994).

[25] Major Craig T. Trebilcock, “The Myth of Posse Comitatus,” Homeland Security Journal, October 2000 at http://www.homelandsecurity.org/journal/articles/Trebilcock.htm, accessed October 22, 2007.

[26] Tom A. Gizzo and Tama S. Monoson, “A Call to Arms: The Posse Comitatus Act and the Use of the Military in the Struggle Against International Terrorism,” 15 PACE INT’L L. REV. 149, 152-53 (Spring 2003).

[27] Linda J. Demaine and Brain Rosen, “Process Dangers of Military Involvement in Civil Law Enforcement: Rectifying the Posse Comitatus Act,” 9 N.Y.U. J. LEGIS. & PUB. POL’Y 167, 176-79 (2005-06); See, e.g., *United States v. Chaparro-Almeida*, 679 F.2d 423 (5th Cir. 1982), cert. denied 459 U.S. 1156 (PCA not violated when defendant seized by Coast Guard); *Gilbert v. United States*, 165 F.3d 470 (6th Cir. 1999) (PCA not violated when National Guard acting as a state marijuana strike force); See also DOD Directive 5525.5, DOD Cooperation With Civilian Law Enforcement Officials, January 15, 1986, Section E4.2, 20-21; See also Gizzo and Monoson, 152-53.

[28] See Mark David Maxwell, “The Enduring Vitality of the Posse Comitatus Act of 1878,” Prosecutor, May/June 2003, 34.

[29] See 329 F. Supp. 916, 923-25 (D.S.D. 1975). This can be described as the “directive active participation” test. See also Maxwell, 35.

[30] *United States v. Jaramillo*, 380 F. Supp. 1375, 1379 (D. Neb. 1974). This can be described as the “pervaded the activities” standard. See Maxwell, 35.

[31] See *United States v. McArthur*, 419 F. Supp. 186, 194 (D.S.D. 1975), aff’d 541 F.2d 1275 (8th Cir. 1976).

[32] See *Bisonette v. Haig*, 776 F.2d 1384, 1387 (8th Cir. 1985); See also Gizzo, 162.

[33] Title 10 U.S. Code, Sec. 375, Restriction on Direct Participation By Military Personnel (1994). DOD Directive 5525.5 also prohibits direct assistance and participation by military personnel in the execution and enforcement of the law.

[34] DoD Directive 5525.5, Secs. E4.1.3 and E4.1.7.2, 17-20.

[35] Demaine and Rosen, 187.

[36] Ibid., 189-190.

[37] Title 6 U.S. Code Sec. 466(b), Sense of Congress Reaffirming the Continued Importance and Applicability of the Posse Comitatus Act (2002). The statute provides: "Congress reaffirms the continued importance of [the PCA], and it is the sense of Congress that nothing in this Act should be construed to alter the applicability of such section to any use of the Armed Forces as a posse comitatus to execute the laws."

[38] Ibid., Sec. 466(a) Findings.

[39] Steven J. Tomisek, "Homeland Security: The New Role for Defense," 189 Strategic Forum 6, February 2002, 4.

[40] DoD Directive 5525.5, Secs. E4.1.2.3.1 and E4.1.2.3.2, 15.

[41] Title 18 U.S. Code, Sec. 831(e)(3), Prohibited Transactions Involving Nuclear Materials (2004).

[42] Maxwell, 35-36. The Military Purpose Doctrine involves actions taken primarily for military or foreign affairs functions such as maintaining discipline on a military base and protecting DoD personnel and equipment.

[43] DoD Directive 5525.5, Sec. E4.1.2, 14-15.

[44] Ibid.

[45] Ibid., Sec. E4.1.2.3.2, 15.

[46] See, e.g., Title 10 U.S. Code, Sec. 374, Maintenance and Operation of Equipment (1988); Title 10 U.S. Code, Sec. 372, Use of Military Equipment and Facilities (1988).

[47] Gizzo and Monoson, 155-57.

[48] A detailed discussion of the 4th Amendment and other Constitutional arguments are beyond the scope of this paper.

[49] President George W. Bush, National Strategy for Homeland Security, Homeland Security Council, October 5, 2007, 2; See also DoD Joint Publication 3-26, Homeland Security, 2 August 2005, I-3.

[50] DoD Joint Publication 3-26, I-2.

[51] President William J. Clinton, Executive Order EO 13010, Critical Infrastructure Protection, July 15, 1996, 1-2.

[52] Presidential Decision Directive (PDD)/NSC-63, Critical Infrastructure Protection, May 22, 1998, Sec. II, 2.

[53] Ibid., Sec. III, 3.

[54] Ibid., Sec. V, 5 and Sec. VII, 7.

[55] Ibid., Sec. VIII, 8 and Annex A, 12-13.

[56] DHS Press Release, "DHS Conducts First Full-Scale Cyber Security Exercise to Enhance Nation's Cyber Preparedness," February 10, 2006, 2.

[57] Statement of Andy Purdy, Acting Director of the National Cyber Security Division (NCSD), DHS Press Conference on the "Cyber Storm" Cyber Security Preparedness Exercise, February 10, 2006, 4.

[58] Ibid.

[59] President George W. Bush, The National Strategy to Secure Cyberspace, February 2003, Executive Summary, viii.

[60] Ibid., Executive Summary, xii-xiii.

[61] Homeland Security Presidential Directive (HSPD)-7, December 17, 2003, Policy, (7)(a)-(f), 2-3.

[62] Ibid., Policy, (16), 3.

[63] Chertoff, 65.

[64] Ibid., 108.

[65] Ibid.

[66] Gordon England, Deputy Secretary of Defense, "Strategy for Homeland Defense and Civil Support," DoD, June 2005, 18.

[67] Ibid.

[68] Rollins and Wilson, 7. This was done by DoD Directive 3020.40, the "Defense Critical Infrastructure Program."

[69] England, 18.

[70] The author recognizes that Computer Network Operations (CNO) is one of the five pillars of Information Operations (IO) recognized by DoD. However, a detailed discussion of CNO, comprised of Computer Network Defense (CND), Computer Network Attack (CNA), and Computer Network Enabling (CNE) operations, and the relationship to IO are beyond the scope

of this paper. For a more detailed discussion of IO and CNO, please reference Joint Publication 3-13, DoD, Information Operations, 13 February 2006.

[71] Clay Wilson, “Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues,” CRS Report for Congress, March 20, 2007, 6.

[72] Ibid., 5.

[73] Ibid., 1.

[74] Donald H. Rumsfeld, Secretary of Defense, The National Defense Strategy of the United States of America, DoD, March 2005, 13.

[75] Rogin, 2.

[76] Donald Rumsfeld, Secretary of Defense, Information Operations Roadmap, DoD, October 2003, Executive Summary, 6.

[77] Rogin, 2.

[78] President George W. Bush, Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001, Sec. 4(b), 2.

[79] Mike Gipson, “USSTRATCOM & DoD’s Efforts to Combat Cyberthreats,” USSTRATCOM/J8A Power Point Brief, 10 August 2006, 7.

[80] USSTRATCOM website at http://www.stratcom.mil/organization-fnc_comp.html, accessed October 25, 2007.

[81] USSTRATCOM Fact Sheet at http://www.stratcom.mil/fact_sheets/fact_jtf_gno_print.html, accessed October 25, 2007.

[82] Ibid.

[83] Ibid.

[84] Rumsfeld, DOD IO Roadmap, 48.

[85] Ibid., 18.

[86] Wilson, 4.

[87] McCaffrey, 5.

[88] Wilson, 5.

[89] DoD Joint Publication 3-26, Executive Summary, ix. Military assistance for civil disturbances is not discussed in detail since it is the least analogous to potential operations in cyberspace.

[90] DoD Directive 3025.15, Military Assistance to Civil Authorities, February 18, 1997, Sec. 1.1, 1.

[91] Ibid., Sec. E2.1.8, 15..

[92] Ibid., Sec. 4.1, 2.

[93] Tomisek, 1.

[94] Ibid., 3; See also DOD Directive 3025.15, , Sec. 4.2, 2-3.

[95] Tomisek, 2.

[96] DoD Joint Publication 3-26, Executive Summary, ix.

[97] DoD Directive 3025.1, Military Support to Civil Authorities, January 15, 1993, Sec. E2.1.21, 21-22.

[98] Ibid., Secs. 4.4.9-4.4.10, 7. Some of the immediate response categories listed in the Directive include emergency restoration of essential public services, interim emergency communications, and facilitating the reestablishment of civil government functions. Ibid., Sec. 4.5.4, 7-8.

[99] Title 10 U.S. Code, Sec. 375.

[100] DoD Joint Publication 3-26, Executive Summary, ix.

[101] DoD Directive 5525.5, Sec. 4, 2.

[102] Ibid., Sec. E2.1.4, 9.

[103] Ibid., Sec. E2.1.8, 10.

[104] Dr. Gregory B. White and Joe H. Sanchez Jr., “Dark Screen Sheds Light on Cyberspace Security Issues,” SIGNAL Magazine, January 2003, 1 (The exercise emphasized communications channels that needed to be in place to share indications and warnings of possible cyberattacks and to conduct timely reporting of actual attacks in progress and involved representatives from federal, state and local government agencies, as well as industry, local military bases and academia).

[105] Ibid., 2.

[106] Patience Wait, “Cyber Storm Exercise Challenged Coordination, Communications,” Government Computer News, September 15, 2006 at http://www.gcn.com/cgi-bin/udt/ m.display.printable? clientid=gcn_daily &ctory.id=42017, accessed November 8, 2007.

[107] Ibid.

[108] DHS Press Release, “DHS Conducts First Full-Scale Cyber Security Exercise to Enhance Nation’s Cyber Preparedness,” February 10, 2006.

[109] DHS, NCSD, Cyber Storm Exercise Report, September 12, 2006, Executive Summary, 1.

[110] Ibid., 11.

[111] Ibid., 14.

[112] Rollins and Wilson, 8.

[113] Ibid.

[114] A detailed discussion of organizational recommendations for DoD and the interagency are beyond the scope of this paper. However, the author contends that a JIATF-Cyberspace should be established at NORTHCOM (national critical infrastructure defense) and STRATCOM (offensive global cyber attack capability) to serve U.S. national security interests.

[115] Matthew Carlton Hammond, The Posse Comitatus Act: A Principle in Need of Renewal, 75 WASH. U.L.Q. 953, 961 (Summer 1997).

[116] Bush, National Strategy for Homeland Security, 48.

[117] Eric Schmitt, “Wider Military Role in the U.S. Is Urged,” N.Y. Times, July 21, 2002, A1.

[118] Sen. John Warner, Chairman, Senate Armed Services Committee Hearing, October 4, 2002.

[119] Demaine and Rosen, 222.

[120] John R. Brinkerhoff, “The Posse Comitatus Act and Homeland Security,” Homeland Security Journal, February 2002, 7.

[121] Gary Felicetti and John Luce, “The Posse Comitatus Act: Setting the Record Straight on 124 Years of Mischief and Misunderstanding Before Any More Damage is Done,” 175 MIL. L. REV. 86, 460 (March 2003).

[122] Even when these critical defense assets are located at public or private sites beyond the direct control of DOD, their protection must be assured on a priority basis. See DoD Joint Publication 3-13, Information Operations, 13 February 2006.

[123] See, e.g., *United States v. Banks*, 539 F.2d 14, *cert. denied* 429 U.S. 1024 (1976).

[124] Christopher J. Schmidt and David A. Klinger, “Altering the Posse Comitatus Act: Letting the Military Address Terrorist Attacks on US Soil,” 39 CREIGHTON L. REV. 667, 682 (April 2006).

[125] Jonathan Marino, Government Executive Daily Briefing, “Panelists: Pentagon Could Take Lead Role in Some Disasters,” November 13, 2006.

[126] Thomas C. Wingfield and James B. Michael, “An Introduction to Legal Aspects of Operations in Cyberspace,” Naval Post Graduate School, 28 April 2004, 10.

[127] DoD Joint Publication 3-26, I-11.

[128] Ibid., III-3.

[129] Geoffrey Klingsporn, “The Secret Posse,” Legal Affairs, March/April 2005, 24-25.

[130] Bush, The National Strategy to Secure Cyberspace, viii.

[131] Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, March 16, 1999, 2.

[132] Rollins and Wilson, 2.

[133] Brewin, 16.

[134] Schmidt and Klinger, 829.

[135] Herbert Lin, “Policy Consequences and Legal/Ethical Implications of Offensive Information Operations and Cyberattack,” Computer Science and Telecommunications Board, National Academies, August 25, 2006, 5.

[136] DoD Joint Publication 3-26, III-3.

[137] Metz, 11.

[138] Schmidt and Klinger, 674-75.

[139] Gizzo and Monoson, 150.

[140] Demaine and Rosen, 180-81.

[141] DoD Joint Publication 3-26, Executive Summary, viii.

[142] Grant, 8.

[143] Stephen Young, “Features - The Posse Comitatus Act: A Resource Guide,” Law and Technology Resources for Legal Professionals, February 17, 2003, 4.